Informe de malware y vulnerabilidades del servidor

Ejemplo de informe de malware y vulnerabilidades del servidor

Informe generado: 25 nov. 2026, 11:16

> Los nombres, archivos y estructuras de directorios de este ejemplo público son ficticios. Se han eliminado el código fuente, los datos de solicitudes, las notas del cliente y los identificadores. Los comentarios se han reescrito; se conservan los recuentos, las evaluaciones y los resultados de revisión.

Resultado actual

Medio

Hallazgos: 213 | Por revisar: 137 | Probablemente inofensivos: 0 | Resueltos, aceptados o ignorados: 76

El riesgo refleja los hallazgos pendientes de revisión. Los que la IA considera probablemente inofensivos se cuentan por separado.

Gravedad	Hallazgos originales	Requieren atención
Crítico	0	0
Alto	6	0
Medio	8	4
Bajo	191	125
Informativo	8	8

Resumen

Este análisis real detectó 213 elementos. Tras la revisión, 137 siguen requiriendo atención: 4 de gravedad media, 125 baja y 8 informativos. Los otros 76 se resolvieron, aceptaron o ignoraron. Las versiones PHP en uso incluyen la corrección de PHP2Shell; las antiguas sin uso aún necesitan limpieza.

Los hallazgos son indicios, no pruebas, y un análisis solo ve lo que esta cuenta puede leer. Ningún análisis puede demostrar que un servidor no haya sido comprometido.

PHP2Shell

Corregido donde se usa

El PHP que usan tus sitios web incluye la corrección. Hay un PHP más antiguo instalado, pero esta cuenta no lo usa: elimínalo cuando puedas.

PHP	Versión	Estado	Corregido en	En uso
/opt/example-php/runtime-01/bin/php	8.2.35	Corregido	8.2.35	Sí
/opt/example-php/runtime-02/bin/php	7.4.33	Sin soporte	-	No
/opt/example-php/runtime-03/bin/php	8.0.30	Sin soporte	-	No
/opt/example-php/runtime-04/bin/php	8.1.34	Sin soporte	-	No
/opt/example-php/runtime-05/bin/php	8.3.36	Corregido	8.3.36	No
/opt/example-php/runtime-06/bin/php	8.4.27	Corregido	8.4.27	No
/opt/example-php/runtime-07/bin/php	8.5.12	Corregido	8.5.12	No

PHP	Versión	Estado	Corregido en	En uso
/opt/example-php/runtime-08/bin/php	7.4.33	Sin soporte	-	No
/opt/example-php/runtime-09/bin/php	8.0.30	Sin soporte	-	No
/opt/example-php/runtime-10/bin/php	8.1.34	Sin soporte	-	No
/opt/example-php/runtime-11/bin/php	8.2.35	Corregido	8.2.35	Sí
/opt/example-php/runtime-12/bin/php	8.3.36	Corregido	8.3.36	No
/opt/example-php/runtime-13/bin/php	8.4.27	Corregido	8.4.27	No
/opt/example-php/runtime-14/bin/php	8.5.12	Corregido	8.5.12	No

En uso: lo que muestran los pools de PHP-FPM, los procesos en ejecución, el comando php y las tareas programadas de esta cuenta. Otra cuenta del mismo servidor aún podría usar un PHP marcado como No.

Comprobaciones

Comprobaciones	Estado
Servidor y sistema operativo	Completada
Panel de alojamiento	Completada
Versiones de PHP	Completada
Paquetes de PHP	Completada
Correcciones de PHP2Shell de la distribución	Completada
Sitios web y aplicaciones	Completada
Ajustes de depuración	Completada
Tareas programadas	Completada
Archivos de inicio de la shell	Completada
Claves SSH	Completada
Servicios de usuario	Completada
Programas de inicio	Completada
Bibliotecas precargadas	Completada
Carpetas temporales	Completada
Procesos en ejecución	Completada
Ganchos de inicio de Python	Completada
Inventario de archivos	Completada
Patrones de código PHP	Completada
Patrones de código Python	Completada
Scripts en un lugar indebido	Completada
Nombres de archivo disfrazados	Completada
PHP oculto en otros tipos de archivo	Completada

Comprobaciones	Estado
Código disfrazado	Completada
Archivos de configuración del servidor	Completada
Archivos expuestos	Completada
Permisos de archivos	Completada
Fechas de archivo alteradas	Completada
Registros de acceso web	Completada
Registros de errores	Completada
Evaluación de PHP2Shell	Completada
Ajuste de progreso de subida de PHP	Completada

Hallazgos (213)

Archivo con nombre de imagen o documento que se ejecuta como PHP (3)

Qué significa: El nombre del archivo tiene dos extensiones (por ejemplo, photo.jpg.php) o disfraza un archivo PHP de archivo multimedia. Es una forma habitual de colar un script a través de los filtros de subida.

Cómo solucionarlo: Elimina el archivo a menos que sepas exactamente por qué existe y, después, revisa el formulario de subida que lo aceptó.

`/home/example-user/archive/sample-188.txt.php`

Alto | Confianza media | Resuelto | Sospechoso (Opinión de la IA (orientativa) #1)

`/home/example-user/archive/sample-189.txt.php`

Alto | Confianza media | Resuelto | Sospechoso (Opinión de la IA (orientativa) #1)

`/srv/example-app/packages/sample-190.txt.php`

Alto | Confianza media | Riesgo aceptado | Requiere investigación (Opinión de la IA (orientativa) #2)

> #### Opinión de la IA (orientativa) #1 - Sospechoso
>
> **Explicación:** La evaluación original de la IA detectó características sospechosas que requerían investigación. Por sí solas no demuestran una intrusión.
>
> **Cómo verificarlo:** Compara el archivo con una versión fiable de la aplicación y revisa su contexto antes de modificarlo.
>
> **Solución:** Elimina el archivo a menos que sepas exactamente por qué existe y, después, revisa el formulario de subida que lo aceptó.
>
> **Evitar que vuelva a ocurrir:** Mantén actualizado el software compatible y compara los cambios inesperados con una referencia fiable.

> #### Opinión de la IA (orientativa) #2 - Requiere investigación
>
> **Explicación:** La evaluación original de la IA no pudo determinar si este elemento era esperado. Revisa las pruebas y el contexto de la aplicación.
>
> **Cómo verificarlo:** Compara el archivo con una versión fiable de la aplicación y revisa su contexto antes de modificarlo.
>
> **Solución:** Elimina el archivo a menos que sepas exactamente por qué existe y, después, revisa el formulario de subida que lo aceptó.
>
> **Evitar que vuelva a ocurrir:** Mantén actualizado el software compatible y compara los cambios inesperados con una referencia fiable.

Código PHP dentro de un archivo que no es PHP (3)

Qué significa: Un archivo con otra extensión (por ejemplo, una imagen, un archivo de texto o un icono) contiene código PHP. Con un servidor mal configurado o una inclusión, puede ejecutarse como script.

Cómo solucionarlo: Examina el archivo en modo de solo lectura. Elimínalo si no es un archivo auténtico y busca el código que lo incluye.

`/srv/example-app/public/media/sample-191.txt`

Alto | Confianza media | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

`/srv/example-app/public/media/sample-192.txt`

Alto | Confianza media | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

`/srv/example-app/public/media/sample-193.txt`

Alto | Confianza media | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

> ### Opinión de la IA (orientativa) #1 - Probablemente inofensivo
>
> **Explicación:** La evaluación original de la IA consideró este elemento probablemente inofensivo en su contexto. Esta opinión no demuestra que un archivo sea seguro.
>
> **Cómo verificarlo:** Compara el archivo con una versión fiable de la aplicación y revisa su contexto antes de modificarlo.
>
> **Solución:** Examina el archivo en modo de solo lectura. Elimínalo si no es un archivo auténtico y busca el código que lo incluye.
>
> **Evitar que vuelva a ocurrir:** Mantén actualizado el software compatible y compara los cambios inesperados con una referencia fiable.

Copia de seguridad o archivo comprimido en la carpeta web pública (6)

Qué significa: Las copias de seguridad, volcados de bases de datos o archivos comprimidos dentro de la carpeta pública a menudo pueden ser descargados por cualquiera que adivine el nombre.

Cómo solucionarlo: Mueve las copias de seguridad fuera de la carpeta pública y elimina las que ya no necesites.

`/srv/example-app/public/sample-001.zip`

Medio | Confianza media | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

`/srv/example-app/public/sample-002.zip`

Medio | Confianza media | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

`/srv/example-app/public/media/sample-003.zip`

Medio | Confianza media | Abierto | Requiere investigación (Opinión de la IA (orientativa) #2)

`/srv/example-app/public/media/sample-004.zip`

Medio | Confianza media | Abierto | Requiere investigación (Opinión de la IA (orientativa) #2)

`/srv/example-app/public/media/sample-005.zip`

Medio | Confianza media | Abierto | Requiere investigación (Opinión de la IA (orientativa) #2)

`/srv/example-app/public/media/sample-006.zip`

Medio | Confianza media | Abierto | Requiere investigación (Opinión de la IA (orientativa) #2)

> ### Opinión de la IA (orientativa) #1 - Probablemente inofensivo
>
> **Explicación:** La evaluación original de la IA consideró este elemento probablemente inofensivo en su contexto. Esta opinión no demuestra que un archivo sea seguro.
>
> **Cómo verificarlo:** Compara el archivo con una versión fiable de la aplicación y revisa su contexto antes de modificarlo.
>
> **Solución:** Mueve las copias de seguridad fuera de la carpeta pública y elimina las que ya no necesites.
>
> **Evitar que vuelva a ocurrir:** Mantén actualizado el software compatible y compara los cambios inesperados con una referencia fiable.

> ### Opinión de la IA (orientativa) #2 - Requiere investigación
>
> **Explicación:** La evaluación original de la IA no pudo determinar si este elemento era esperado. Revisa las pruebas y el contexto de la aplicación.
>
> **Cómo verificarlo:** Compara el archivo con una versión fiable de la aplicación y revisa su contexto antes de modificarlo.
>
> **Solución:** Mueve las copias de seguridad fuera de la carpeta pública y elimina las que ya no necesites.
>
> **Evitar que vuelva a ocurrir:** Mantén actualizado el software compatible y compara los cambios inesperados con una referencia fiable.

Paquete de páginas de error para desarrollo instalado (1)

Qué significa: Hay instalado un paquete de páginas de error de desarrollo (como Laravel Ignition). Las versiones antiguas tenían fallos graves, y las páginas de depuración revelan detalles.

Cómo solucionarlo: Instala solo las dependencias de producción (composer install --no-dev) o actualiza el paquete, y mantén desactivado el modo de depuración.

`/srv/example-app/packages/sample-007.php`

Medio | Confianza media | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

> ### Opinión de la IA (orientativa) #1 - Probablemente inofensivo
>
> **Explicación:** La evaluación original de la IA consideró este elemento probablemente inofensivo en su contexto. Esta opinión no demuestra que un archivo sea seguro.
>
> **Cómo verificarlo:** Compara el archivo con una versión fiable de la aplicación y revisa su contexto antes de modificarlo.
>
> **Solución:** Instala solo las dependencias de producción (composer install --no-dev) o actualiza el paquete, y mantén desactivado el modo de depuración.
>
> **Evitar que vuelva a ocurrir:** Mantén actualizado el software compatible y compara los cambios inesperados con una referencia fiable.

Programa en ejecución cuyo archivo se eliminó (1)

Qué significa: Un proceso propiedad de esta cuenta se está ejecutando desde un archivo que ya no existe. Las actualizaciones de software pueden causarlo, pero el malware también se elimina a sí mismo tras iniciarse.

Cómo solucionarlo: Identifica el proceso con ps y detenlo si no lo reconoces.

`/srv/example-workers/sample-213.bin`

Medio | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

> ### Opinión de la IA (orientativa) #1 - Probablemente inofensivo
>
> **Explicación:** La evaluación original de la IA consideró este elemento probablemente inofensivo en su contexto. Esta opinión no demuestra que un archivo sea seguro.
>
> **Cómo verificarlo:** Compara el archivo con una versión fiable de la aplicación y revisa su contexto antes de modificarlo.
>
> **Solución:** Identifica el proceso con ps y detenlo si no lo reconoces.
>
> **Evitar que vuelva a ocurrir:** Mantén actualizado el software compatible y compara los cambios inesperados con una referencia fiable.

Las fechas del archivo parecen alteradas (153)

Qué significa: La hora de cambio de estado del archivo (ctime) es mucho más reciente que su hora de modificación (mtime). Los atacantes suelen retrasar las fechas de modificación para que un archivo colocado se confunda con los más antiguos; las restauraciones y algunas herramientas de despliegue también pueden causarlo.

Cómo solucionarlo: Comprueba quién cambió el archivo y cuándo. Si nadie de tu lado lo hizo, revisa su contenido.

`/srv/example-app/packages/sample-008.php`

Bajo | Confianza baja | Abierto

`/srv/example-app/packages/sample-009.php`

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-010.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-011.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-012.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-013.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-014.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-015.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-016.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-017.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-018.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-019.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-020.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-021.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-022.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-023.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-024.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-025.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-026.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-027.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-028.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-029.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-030.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-031.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-032.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-033.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-034.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-035.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-036.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-037.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-038.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-039.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-040.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-041.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-042.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-043.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-044.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-045.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-046.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-047.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-048.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-049.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-050.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-051.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-052.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-053.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-054.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-055.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-056.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-057.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-058.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-059.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-060.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-061.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-062.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-063.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-064.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-065.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-066.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-067.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-068.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-069.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-070.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-071.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-072.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-073.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-074.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-075.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-076.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-077.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-078.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-079.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-080.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-081.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-082.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-083.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-084.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-085.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-086.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-087.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-088.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-089.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-090.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-091.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-092.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-093.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-094.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-095.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-096.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-097.php

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/srv/example-app/packages/sample-098.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-099.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-100.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-101.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-102.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-103.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-104.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-105.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-106.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-107.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-108.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-109.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-110.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-111.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-112.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-113.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-114.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-115.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-116.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-117.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-118.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-119.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-120.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-121.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-122.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-123.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-124.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-125.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-126.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-127.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-128.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-129.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-130.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-131.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-132.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-133.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-134.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-135.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-136.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-137.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-138.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-139.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-140.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-141.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-142.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-143.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-144.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-145.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-146.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-147.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-148.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-149.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-150.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-151.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-152.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-153.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-154.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-155.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-156.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-157.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-158.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-159.php

Bajo | Confianza baja | Abierto

/srv/example-app/packages/sample-160.php

Bajo | Confianza baja | Abierto

> ### Opinión de la IA (orientativa) #1 - Probablemente inofensivo
>
> **Explicación:** La evaluación original de la IA consideró este elemento probablemente inofensivo en su contexto. Esta opinión no demuestra que un archivo sea seguro.
>
> **Cómo verificarlo:** Compara el archivo con una versión fiable de la aplicación y revisa su contexto antes de modificarlo.
>
> **Solución:** Comprueba quién cambió el archivo y cuándo. Si nadie de tu lado lo hizo, revisa su contenido.
>
> **Evitar que vuelva a ocurrir:** Mantén actualizado el software compatible y compara los cambios inesperados con una referencia fiable.

Solicitudes con datos que parecen un ataque (27)

Qué significa: Tus registros de acceso contienen solicitudes con cargas típicas de ataque. La mayoría son sondeos automáticos que fallan; aparecen para dar contexto.

Cómo solucionarlo: No es necesario hacer nada a menos que alguna solicitud coincidente tuviera éxito. Mantén tu software actualizado.

/var/log/example-app/sample-161.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-162.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-163.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-164.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-165.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-166.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-167.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-168.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-169.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-170.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-171.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-172.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-173.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-174.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-175.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-176.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-177.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-178.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-179.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-180.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

/var/log/example-app/sample-181.log

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

`/var/log/example-app/sample-182.log`

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

`/var/log/example-app/sample-183.log`

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

`/var/log/example-app/sample-184.log`

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

`/var/log/example-app/sample-185.log`

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

`/var/log/example-app/sample-186.log`

Bajo | Confianza baja | Ignorado | Probablemente inofensivo (Opinión de la IA (orientativa) #1)

`/var/log/example-app/sample-187.log`

Bajo | Confianza baja | Abierto

> ### Opinión de la IA (orientativa) #1 - Probablemente inofensivo
>
> **Explicación:** La evaluación original de la IA consideró este elemento probablemente inofensivo en su contexto. Esta opinión no demuestra que un archivo sea seguro.
>
> **Cómo verificarlo:** Compara el archivo con una versión fiable de la aplicación y revisa su contexto antes de modificarlo.
>
> **Solución:** No es necesario hacer nada a menos que alguna solicitud coincidente tuviera éxito. Mantén tu software actualizado.
>
> **Evitar que vuelva a ocurrir:** Mantén actualizado el software compatible y compara los cambios inesperados con una referencia fiable.

Código muy camuflado (4)

Qué significa: El archivo contiene cadenas codificadas largas, texto construido carácter a carácter o un camuflaje similar. Puede ser la protección anticopia de un plugin de pago o malware que oculta su propósito.

Cómo solucionarlo: Compara el archivo con la copia del proveedor. Los archivos camuflados desconocidos en una carpeta del sitio deberían ser revisados por alguien que conozca la aplicación.

`/srv/example-app/packages/sample-194.php`

Bajo | Confianza baja | Abierto

`/srv/example-app/packages/sample-195.php`

Bajo | Confianza baja | Abierto

`/srv/example-app/packages/sample-196.php`

Bajo | Confianza baja | Abierto

`/srv/example-app/packages/sample-197.php`

Bajo | Confianza baja | Abierto

PHP antiguo instalado que tus sitios no usan (6)

Qué significa: Este PHP no tiene soporte, es anterior a la corrección de PHP2Shell o no se pudo confirmar su corrección, pero nada en esta cuenta lo usa: ningún pool de PHP-FPM, ningún proceso en ejecución, ningún comando php ni ninguna tarea programada. Con la configuración actual no puede servir tus sitios web, así que tiene gravedad baja. Otra cuenta del mismo servidor aún podría usarlo.

Cómo solucionarlo: Elimínalo si nada lo necesita (tu proveedor de alojamiento o tu panel de control puede desinstalar una versión de PHP) y no cambies ningún sitio a esa versión.

/opt/example-php/sample-198.php

Bajo | Confianza media | Abierto

/opt/example-php/sample-199.php

Bajo | Confianza media | Abierto

/opt/example-php/sample-200.php

Bajo | Confianza media | Abierto

/opt/example-php/sample-201.php

Bajo | Confianza media | Abierto

/opt/example-php/sample-202.php

Bajo | Confianza media | Abierto

/opt/example-php/sample-203.php

Bajo | Confianza media | Abierto

El seguimiento del progreso de subida de PHP está activado (1)

Qué significa: session.upload_progress.enabled está activado. Los problemas de PHP2Shell afectan a esta función, así que desactivarla reduce la exposición si no la usas.

Cómo solucionarlo: Establece session.upload_progress.enabled = Off en php.ini o .user.ini si tus sitios no muestran el progreso de subida.

/etc/example-php/sample-212.ini

Bajo | Confianza media | Abierto

PHP incluye la corrección de PHP2Shell (8)

Qué significa: Este PHP está en la versión corregida o en una posterior, o el paquete de su proveedor confirma la corrección.

Cómo solucionarlo: No es necesario hacer nada respecto a PHP2Shell para este PHP.

/opt/example-php/sample-204.php

Informativo | Confianza alta | Abierto

/opt/example-php/sample-205.php

Informativo | Confianza alta | Abierto

/opt/example-php/sample-206.php

Informativo | Confianza alta | Abierto

/opt/example-php/sample-207.php

Informativo | Confianza alta | Abierto

/opt/example-php/sample-208.php

Informativo | Confianza alta | Abierto

/opt/example-php/sample-209.php

Informativo | Confianza alta | Abierto

/opt/example-php/sample-210.php

Informativo | Confianza alta | Abierto

/opt/example-php/sample-211.php

Informativo | Confianza alta | Abierto